II. ИНСТИТУЦИОНАЛИЗАЦИЯ ЭКОНОМИКИ: ПРОБЛЕМЫ И РЕШЕНИЯ

УДК 338.23

J.Neumeier, K. Lemaire, A.P.Taburchak, A.L.Zelezinskii

SOCIAL ENGINEERING, IMPERFECT HUMAN

The article introduces the concept of "Social Engineering". This term is used for a broad range of malicious activities accomplished through human interactions. The previous year has seen an enormous increase in the studies related to social engineering. This increase is partly due to the increasing number of social engineering attacks and partly due to people's inability to identify the attack. The authors define the subject of social engineering from a Cyber Security professional perspective. A literature review from the information technology, psychology, and business disciplines explains the interconnected nature of the topic as well as the necessity to comprehend it from multiple viewpoints. The article presents several case studies of successful attacks performed as well as their efficacy.

Keywords: Social Engineering; Information Security; Psychology of Information Security; Ethics; Threat Agent.

Ж.Нумьер[1], К.Люмер[2], А.П.Табурчак[3], А.Л.Зелезинский[4]

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ, НЕСОВЕРШЕННЫЙ ЧЕЛОВЕК

В статье вводится понятие "Социальная инженерия". Этот термин используется для обозначения широкого спектра вредоносных действий, совершаемых посредством взаимодействия с людьми. В прошлом году наблюдался огромный рост исследований, связанных с социальной инженерией. Это увеличение частично связано с увеличением числа атак социальной инженерии и частично из-за неспособности людей идентифицировать атаку. Авторы определяют предмет социальной инженерии с профессиональной точки зрения кибербезопасности. Обзор литературы по информационным технологиям, психологии и бизнес-дисциплинам объясняет взаимосвязанный характер темы, а также необходимость осмысления её с разных точек зрения. В статье представлено несколько примеров успешно проведённых атак, а также их эффективность.

Ключевые слова: социальная инженерия; информационная безопасность; психология информационной безопасности; этика; агент угрозы.

DOI: 10.36807/2411-7269-2022-2-29-11-16

1.Introduction

The COVID-19 pandemic has greatly changed the way people work driving the massive use of remote working, which had an impact on the use of cloud services. It has been reflected in the adoption of business collaborative platforms (such as Microsoft Teams), the opening of companies' private networks (through VPNs for example), as well as the migration of corporate

[1] Нумьер Ж., аспирант Технологического института Труа, г. Труа (Франция)
Neumeier J., Postgraduate of the Institute of Technology of Troyes, Troyes (France)
E-mail: jean.neumeier34@gmail.com

[2] Люмер К., аспирант Технологического института Труа, г. Труа (Франция)
K. Lemaire, Postgraduate of the Institute of Technology of Troyes, Troyes (France)
E-mail: kevin.lemaire51@gmail.com

[3] Табурчак А.П., Декан факультета экономики и менеджмента, доктор экономических наук, профессор; Федеральное государственное бюджетное образовательное учреждение высшего образования "Санкт-Петербургский государственный технологический институт (технический университет)", г. Санкт-Петербург
Taburchak A.P., Decan of the Faculty of Economics and Management, Doctor of Economics, Professor; Federal State Budgetary Educational Institution of Higher Education "Saint-Petersburg State Technological Institute (Technical University)", Saint-Petersburg
E-mail: ta@inbox.ru

[4] Зелезинский А.Л., доцент кафедры менеджмента и маркетинга, кандидат педагогических наук, доцент; ФГБОУ ВО "Санкт-Петербургский государственный технологический институт (технический университет)", г Санкт-Петербург
Zelezinskii A.L., Associate Professor of the Department of Management and Marketing, PhD in Pedagogics, Associate Professor; Federal State Budgetary Educational Institution of Higher Education "Saint-Petersburg State Technological Institute (Technical University)", Saint-Petersburg
E-mail: uchposob@yandex.ru

services and applications to the Cloud. Mechanically, the attack surface of companies' Information System has been enlarged and this trend has been accompanied by a record increase in cyber-attacks between January and April 2020. The generalisation of basic but efficient protective measures (double authentication, HTTPS encryption, awareness training) pushes malicious actors to exploit human-related vulnerabilities instead of technical vulnerabilities.

Social engineering can be defined as the act of manipulating human beings, most often with the use of psychological persuasion, to gain access to systems containing data, documents, and information that the social engineer should not have access to obtain.

Various forms of social engineering can be found throughout history but considering the increased use of technology in today's world in every aspect of life, the threat continues to grow and develop into a complex process that can be difficult to stop. In fact, social engineering can be considered one of the leading threats to information security today.

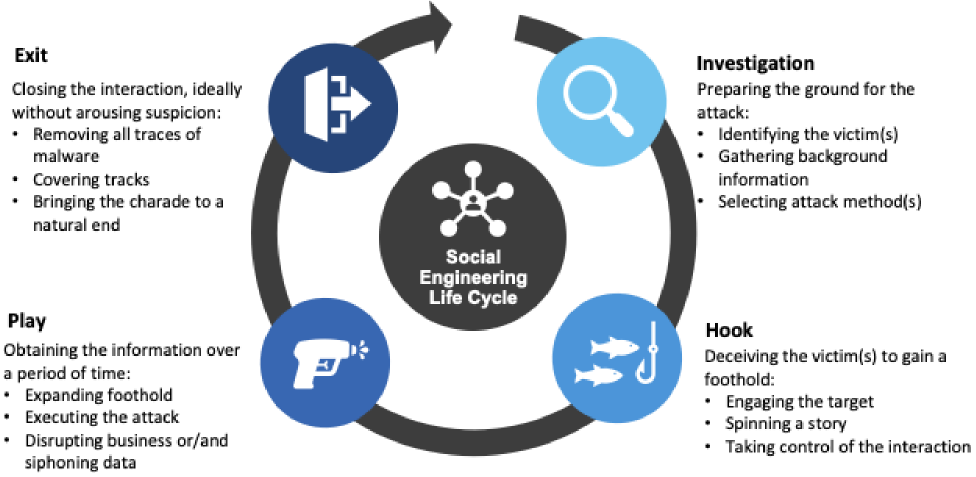
Exit
Closing the interaction, ideally without arousing suspicion:
• Removing all traces of malware
• Covering tracks
• Bringing the charade to a natural end
Investigation
Preparing the ground for the attack:
• Identifying the victim(s)
• Gathering background information
• Selecting attack method(s)
Social Engineering Life Cycle
Play
Obtaining the information over a period of time:
• Expanding foothold
• Executing the attack
• Disrupting business or/and siphoning data
Hook
Deceiving the victim(s) to gain a foothold:
• Engaging the target
• Spinning a story
• Taking control of the interaction

Figure 1 – Social Engineering Attack Lifecycle

What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

There are two main categories under which all social engineering attempts could be classified:

1. Computer or technology-based deception: The technology-based approach is to deceive the user into believing that he is interacting with the real computer system and get him to provide confidential information.

2. Human based deception: This is done through deception, by taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked. [5]

Attack process

1.Social Engineering susceptibility

Social engineering researchers still struggle to suggest a framework based on the susceptibility for an organisation to be subject to Social Engineering attacks.

The following diagram illustrates a suggested framework for future research on the topic of social engineering that is flexible enough to allow for a variety of theories from different disciplines to converge in a robust analysis of social engineering.

An essential element of all social engineering is the idea of ethics, and this diagram provides for ethical consideration at each discipline component. At the root of the framework, is determining social engineering susceptibility at the organisational level.

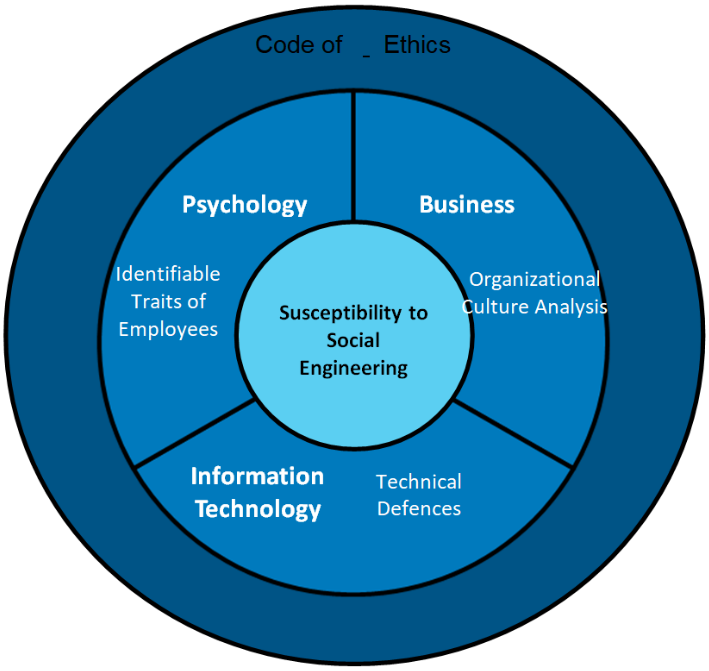
Code of _ Ethics
Psychology
Business
Identifiable Traits of Employees
Susceptibility to Social Engineering
Organizational Culture Analysis
Information Technology
Technical Defences

Figure 2 – Social Engineering susceptibility research framework with specific concepts from the disciplines

Each of the concepts or theories from the disciplines are beneficial from a social engineering mitigation perspective, but collectively, the three disciplines (Psychology, Business, Information Technology) provide a powerful framework within which to view and analyse susceptibility.

More importantly, they also provide direct and immediate feedback to organisations so they can determine what their weaknesses are and where they are located so appropriate decisions can be made to strengthen any of the weakened areas.

2.Attacks type

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the five most common forms of digital social engineering assaults.

Baiting

As its name implies, baiting attacks use a false promise to pique a victim’s greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait – typically malware-infected flash drives – in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company’s payroll list.

Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.

Baiting scams don’t necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

Scareware

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraud ware.

A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you or will direct you to a malicious site where your computer becomes infected.

Scareware is also distributed via spam email that doles out bogus warnings or makes offers for users to buy worthless/harmful services.

Pretexting

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim to perform a critical task.

The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexted asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.

All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Phishing

As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity, or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website – nearly identical in appearance to its legitimate version – prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.

Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting, and blocking them are much easier for mail servers having access to threat sharing platforms.

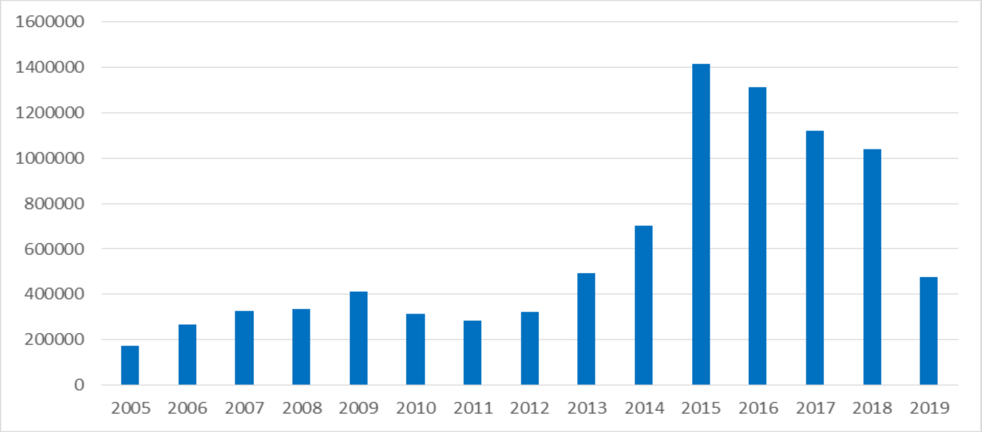

Figure 3 – Table of the total number of unique phishing reports (campaigns) received according to APWG [1]

Spear phishing

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skilfully.

A spear phishing scenario might involve an attacker who, in impersonating an organisation's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

Combined attacks

The types of attacks mentioned above are often combined and used together for an extended period by attackers to gain information and analyse a company's business process.

The final goal is often to bypass the security measures in place and gain some level of access to corporate resources but not always.

For instance, in early 2020, three private equity companies lost $1.3 million. There was an electronic transfer of a total of $1.3 million to the bank accounts that hackers had access to - while executives thought they had reached an investment agreement with start-ups. The attack unfolds in 4 parts:

1. Launch of a phishing campaign to retrieve staff access and analyse how the

business works.

2. Recognition and learning of internal business mechanisms. Adding rules in bank and companies' mailboxes to hide genuine mails and only show hacker's mails.
3. Interception and transfer by hackers of emails between the bank and the companies.
4. Insertion of fraudulent banking data into email exchanges to retrieve money.

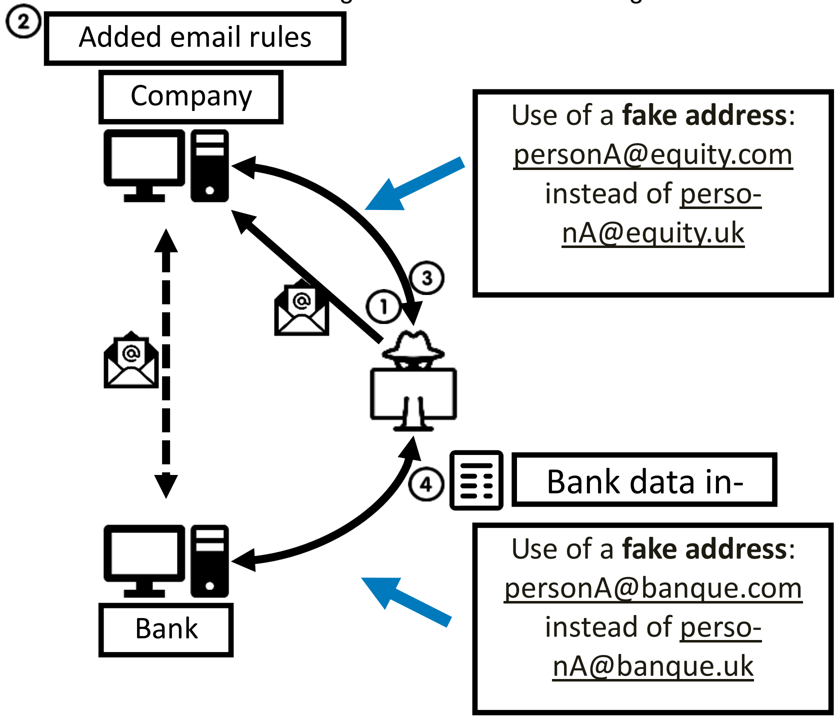

Figure 4 – Example of combined attacks [2]

II. Prevention

Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or when you come across stray digital media lying about. Being alert can help you protect yourself against most social engineering attacks taking place in the digital realm. Moreover, the following tips can help improve your vigilance in relation to social engineering hacks.

- **Don't open emails and attachments from suspicious sources** – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all the time; even an email purportedly coming from a trusted source may have been initiated by an attacker.
- **Use multifactor authentication** – One of the most valuable pieces of information attackers seek are user credentials. Using multi factor authentication helps ensure your account's protection in the event of system compromise.
- **Be wary of tempting offers** – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.
- **Keep your antivirus/antimalware software updated** – Make sure automatic updates are engaged or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied and scan your system for possible infections.

III. Case studies

Twitter

On July 15, 2020, Twitter suffered a breach that combined elements of Social Engineering (security) and phishing. A 17-year-old hacker and accomplices set up a fake website resembling Twitter's internal VPN provider used by employees working from home.

Individuals posing as helpdesk staff called multiple Twitter employees, directing them to submit their credentials to the fake VPN website. Using the details supplied by the unknowing employees, they were then able to seize control of several high-profile user accounts, including **Barack Obama**, **Elon Musk**, **Joe Biden** and **Apple Inc.'s** company account.

The hackers sent messages to Twitter followers soliciting Bitcoin promising double the transaction value in return, collecting some $117,000 in the first 3 hours of the ruse.

Twitter employees were the company's biggest weakness, falling for social engineering exploits that allowed the bad actors a backdoor into highly sensitive login information.

Since the attack, Twitter has vowed to make several crucial vulnerability improvements, including a heavy focus on heightening their detection and monitoring capabilities, access management processes and authentication systems, and more.

Google & Facebook

The biggest social engineering attack of all time (as far as we know) was perpetrated by Lithuanian national Evaldas Rimasauskas against two of the world's biggest companies: Google and Facebook.

Rimasauskas and his team set up a fake company, pretending to be a computer manufacturer that worked with Google and Facebook. Rimsauskas also set up bank accounts in the company's name.

The scammers then sent phishing emails to specific Google and Facebook employees, invoicing them for goods and services that the manufacturer had genuinely provided – but directing them to deposit money into their fraudulent accounts.

Between 2013 and 2015, Rimasauskas and his associates cheated the two tech giants out of over $100 million.

Shark Tank

Shark Tank television judge Barbara Corcoran was tricked in a nearly USD 400,000 phishing and social engineering scam in 2020. A cybercriminal impersonated her assistant and sent an email to the bookkeeper requesting a renewal payment related to real estate investments. He used an email address like the legitimate one. The fraud was only discovered after the bookkeeper sent an email to the assistant's correct address asking about the transaction.

IV. Conclusion

Social engineering has been identified as the most significant threat in the information security field today. One of the most alarming aspects of social engineering is that no one is immune from its effects. A company is only as strong as the most vulnerable individual employed there, and with some businesses containing thousands of employees, the threat is daunting and very real.

Social engineering is best understood from an interdisciplinary perspective, specifically the information technology, psychology, and business disciplines. This integrated approach helps to address the idea of a converged threat that is a major concern for businesses today. The increased use of technology and the interdependence that is seen in the business world today support the idea that social engineering will continue to be a threat for organisations of all types.

It is imperative that research continues this topic considering the increased use of social engineering attacks during the COVID-19 pandemic, and the subject can only truly be understood when viewed from a variety of disciplines.

References

1. APWG | Anti-Phishing Working Group, 6 February 2022, Website, Online: https://apwg.org/.

2. CISO Mag | Hackers Trick Three UK Private Equity Firms into Transferring $1.3 Mn Via BEC Attack, 6 February 2022, Website, online: https://cisomag.eccouncil.org/hackers-trick-three-uk-private-equity-firms-into-transferring-1-3-mn-via-bec-attack/.

3. Wikipedia | Social Engineering, 22 January 2022, Website, online: https://en.wikipedia.org/wiki/Social_engineering_(security).

4. Wikipedia | Phishing, 23 January 2022, Website, online: https://en.wikipedia.org/wiki/Phishing.

5. Abass 2018 | Social Engineering threat and defence: A literature survey, 7 February 2022, Article, Available.